REMARKS

Claim 1 has been amended to clarify the subject matter regarded as the invention. Claims 1-11, 13, 15-17, 19-21, 23-26 are pending.

New claims 25 and 26 have been added. Support for the new claims may be found, as an example and without limitation, at p29-32 of the specification.

The Examiner has rejected claims 1-2, 10, 11, 13, 15-17, 19-21 under 35 U.S.C. 103(a) as being unpatentable over I'Anson, further in view of Park and Shanklin. The rejection is respectfully traversed.

Applicants respectfully submit that since Park is not analogous prior art, the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would not have been obvious at the time the invention was made to a person having ordinary skill in the art under 35 U.S.C. 103. In order to rely on a reference as a basis for rejection of an applicant's invention, the reference must either be in the field of applicant's endeavor or, if not, then be reasonably pertinent to the particular problem with which the invention was concerned. *In re Oetiker*, 977 F.2d 1443, 1446 (Fed. Cir. 1992). The application relates to computer network security, specifically protocol analysis for security-related events. Park, on the other hand, teaches a Distributed Shared Memory (DSM) system for bulk data transfer, and more particularly, to a communication protocol to transfer/receive data between receptive nodes (Park 1:9-12). The objects of Park's invention include: to provide a new Adaptive Granularity type communication protocol to integrate fine and coarse communication in a distributed shared memory (2:46-52), to provide a bulk data communication method for reducing false sharing when the ownership of the block is changed (3:17-21), and to provide a data communication method from home node to local or remote nodes for reading/writing data between memories in a distributed shared memory system in which a plurality of nodes are connected on interconnection network (3:22-30). As such, Park's invention is unrelated to computer network security and is in a field of endeavor different from that of the applicants.

Further, the present application addresses the need for a way to efficiently model normal and valid protocol streams and to detect when an actual protocol stream deviates from the normal

and valid behavior in a way that may indicate that an attack is taking place. Park addresses a different problem, described as follows:

> Distributed Shared Memory system is a multiprocessor computer system in which respective node can refer to memory of other nodes (i.e., distributed memory) as if it were its own memory. This architecture is a cache coherence management basis DSM system. Hence, one node in cache coherence management basis DSM system can refer to the memory of other nodes. It means that DSM system makes it possible to obtain good performance by storing the block referred to the memory of remote nodes in its cache and referring to the data in its cache without direct referring to the memory of remote nodes when it is necessary to refer to the above certain block. However, if the corresponding cache line of certain node are [sic] modified by the certain node when the respective nodes share the memory block of home node, then the nodes with unchanged data are forced to refer to the old, unchanged data. Therefore, implementing cache in respective node introduces problem. (Park 1:32-50)

Park's invention, which addresses cache coherency problems in high performance DSM systems, is not concerned with analyzing data packets for security-related events. Park, therefore, is not pertinent to the protocol analysis / data security problem with which the present application is concerned.

In all, Park's invention is in a field of endeavor different from that of the applicants, and is not pertinent to the problem with which the present application is concerned. As such, it is believed that Park is not analogous prior art.

Applicants further respectfully submit that even if Park could be considered as analogous art, the prior art references when combined do not teach or suggest all the claim limitations. With respect to Claim 1, neither I'Anson, nor Park, nor Shanklin, teaches or suggests "expressing a plurality of invalid transitions from the first state to the invalid state as a plurality of regular expressions", and "applying to a received packet associated with the connection: the plurality of regular expressions to determine whether the packet is associated with one of a plurality of invalid transitions." Specifically, neither I'Anson and Shanklin teaches invalid transitions from a first valid state to an invalid state. Although Park teaches an "INVALID" state, Park does not teach expressing any invalid transition from a valid state to the invalid state as a regular expression. Further, Park's cache states show only a single transition wherever a first valid state (such as "READ ONLY" or "READ WRITE") enters the INVALID state (See Park FIG. 2), and not a plurality of invalid transitions from the first state to the invalid state.

Compare, e.g., Application p. 29, ll. 6-38, and p32, ll. 1-5. Thus, the prior art references do not teach or suggest all the claim limitations when combined. As such, Claim 1 is believed to be allowable.

Claims 2-11, 13, 15-17, and 23-26 depend from Claim 1 and are believed to be allowable for the same reasons described above.

Similarly, Claims 19, 20 and 21 are believed to be allowable for the same reasons described above.

Reconsideration of the application and allowance of all claims are respectfully requested based on the preceding remarks. If at any time the Examiner believes that an interview would be helpful, please contact the undersigned.

Respectfully submitted,

Dated: 2/16/07

Diana Y. Fu
Registration No. 52,924
V 408-973-2593
F 408-973-2595

VAN PELT, YI & JAMES LLP
10050 N. Foothill Blvd., Suite 200
Cupertino, CA 95014